# Amélioration du niveau de sécurité des systèmes à microprocesseur par application du concept de redondance

## 1re partie

**Le concept de redondance existe depuis bien longtemps dans des domaines aussi variés que la mécanique, l'hydraulique, le pneumatique ou l'électrique; avec l'avènement des circuits à microprocesseurs, les concepteurs et utilisateurs l'utilisent à présent pour améliorer le niveau de sécurité des systèmes électroniques. La première partie de cet article est un recensement des différents cas de redondance rencontrés dans les systèmes à microprocesseur; une étude détaillée est effectuée sur les architectures de systèmes devant fonctionner en sécurité positive, la notion de disponibilité de systèmes n'étant ici citée que pour mémoire.**

**B. Kopka et J.-P. Gérardin**
INRS, Centre de Recherche
Département « Ergonomie-Sécurité »
Section « Électronique-Sécurité de Systèmes »
BP 27, 54501 Vandœuvre Cedex

**Improving the safety level of programmable electronic systems by application of the concept of redundancy**

*The concept of redundant design has long been present within the various technical disciplines such as mechanics, hydraulics, or electricity. With the advent of microprocessor circuits, designers and users now make use of redundancy to improve the safety level of electronic systems.*
*This first part of this article is a listing of the different cases of redundancy applicable to programmable electronic systems.*
*A detailed reviews is given of the system architectures which must have fail safe operation. System availability is mentioned only as a reminder.*

## Introduction

Ce n'est pas l'avènement de l'électronique depuis quelques décennies qui a créé le concept de redondance, celui-ci existe depuis bien longtemps et a été mis en œuvre dans des domaines variés utilisant la mécanique, l'hydraulique, le pneumatique ou l'électrique.

Avec l'apparition sur le marché depuis quelques années des systèmes à microprocesseur, la redondance a trouvé un nouveau domaine d'application, son rôle étant toujours de permettre à un dispositif d'effectuer une mission donnée malgré la présence de défaillances internes.

Avant de développer plus en détail le sujet de ce document, il est bon de rappeler brièvement quelques définitions d'usage courant :
– **fiabilité :** aptitude d'un dispositif à assurer une fonction imposée, dans des conditions données, pendant une durée donnée [1];
– **disponibilité :** aptitude d'un dis-

positif à remplir sa fonction requise à un instant donné ou pendant une période de temps donnée [2];
– **sécurité :** absence de circonstance susceptible d'occasionner, soit accident ou mort du personnel, soit dégradation ou perte d'équipement ou de bien [3];
– **sécurité positive :** conception de dispositif telle qu'une défaillance n'altère pas la sécurité :
• une simple défaillance ne doit pas être la cause de dégradation du niveau de sécurité du système,
• une défaillance non détectée ne doit pas, en conjonction avec l'arrivée d'une deuxième défaillance, être la cause de risque supplémentaire;
– **sécurité intrinsèque :** un composant est dit à sécurité intrinsèque lorsqu'il est capable de détecter ses propres défaillances ou lorsque ces dernières sont telles qu'elles provoquent toujours le même comportement du composant.

L'électronique a évolué considérablement depuis quelques années grâce notamment à la création de circuits électroniques à très large échelle d'intégration (VLSI). De ce fait, des domaines industriels aussi variés que la robotique, la chimie, le nucléaire ou des secteurs tels que les banques voient petit à petit leur structure se modifier grâce à l'apparition de systèmes à microprocesseur; de même, cette nouvelle électronique s'installe de plus en plus dans les foyers et l'on peut la trouver sous différentes formes allant des applications ménagères aux loisirs.

L'électronique traditionnelle à éléments discrets (transistors, diodes...) tend à disparaître de plus en plus de ces applications et avec elle son avantage fondamental : la connaissance de ses modes de défaillances. En effet, avec l'avènement des systèmes à microprocesseur sont apparus des modes de défaillances multiples et complexes difficilement appréhendables et qui sont un peu la contrepartie de leurs nombreux avantages :
– la miniaturisation des composants électroniques permet d'implanter ces systèmes pratiquement partout et cela avec un coût total allant en diminuant,
– la puissance de calcul et l'utilisation de mémoires à grande capacité de stockage autorisent des calculs complexes dans tous les domaines,
– une grande souplesse d'utilisation les rend facilement modifiables donc adaptables à tout type de problème,
– la fiabilité globale d'un tel système est supérieure à celle d'un système équivalent réalisé en électro-

*Figure 1 :* Arbre regroupant les différents cas de redondance de l'organe de traitement.
*Tree which subdivides the different cases of redundant information processing elements.*

- REDONDANCE
  - Massive
    - Sans contrôle
      - Homogène
      - Hétérogène
    - Avec contrôle
      - Comparateur
        - Homogène
        - Hétérogène
      - Voteur
        - Homogène
        - Hétérogène
  - Sélective
    - Active
      - Homogène
      - Hétérogène
    - Passive
      - Tiède
        - Homogène
        - Hétérogène
      - Froide
        - Homogène
        - Hétérogène

Ce type d'arbre s'applique à une redondance matérielle ou logicielle, globale ou locale.

*Figure 2 :* Architectures de systèmes utilisant la redondance à des fins de sécurité et/ou disponibilité.
*System architectures which use redundancy for safety and/or availability.*

| Architecture | Désignation | Spécification | Référence |
|---|---|---|---|
| e1, e2 → S | Redondance massive sans contrôle<br><br>e1 = e2 : homogène<br>e1 ≠ e2 : hétérogène | Il s'agit d'un doublage pur et simple. Les deux unités e1 et e2 assurent la réalisation de la mission en même temps; la défaillance d'une chaîne est masquée par le fonctionnement de la seconde. Ce type d'architecture est utilisé pour assurer la disponibilité d'un système. Associée à un dispositif d'auto-contrôle, elle est parfois utilisée pour assurer la sécurité. | 1 |
| e1, e2 → Comparateur → S | Redondance massive avec contrôle par comparateur<br><br>e1 = e2 : homogène<br>e1≠ e2 : hétérogène | Les deux unités e1 et e2 assurent toutes deux la réalisation de la mission; le test des résultats de sortie est assuré par un comparateur qui met le système dans un état de sécurité lors de toute divergence entre les deux chaînes.<br>Ce type d'architecture est utilisé pour assurer la sécurité d'un système. | 2 |
| e1, ep, en → Voteur → S | Redondance massive avec contrôle par voteur<br><br>Voteur p parmi n avec p > n/2<br><br>e1 = e2 = ... = ep = ... = en : homogène<br>e1 ≠ e2 ≠ ... ≠ ep ≠... ≠ en : hétérogène | Chaque unité ei assure la réalisation de la mission; un voteur effectue le contrôle des résultats de sortie fournis par les différentes chaînes. Il fournit une sortie relative à p résultats identiques parmi n possibles : si plus de (n-p) résultats de sortie divergent, le système est mis dans un état de sécurité.<br>Ce type d'architecture est utilisé pour assurer la disponibilité et la sécurité d'un système. | 3 |

nique traditionnelle.

Cette liste d'avantages est non exhaustive; on peut toutefois conclure en remarque générale que les systèmes à microprocesseur ont des encombrements de plus en plus faibles pour des capacités de traitement de plus en plus grandes. Cependant le manque de connaissances concernant les différents types de défaillances pouvant survenir dans les circuits intégrés remet en cause le facteur « sécurité ».

Dans le cadre d'études relatives à la sécurité du personnel, l'I.N.R.S. poursuit actuellement une analyse de la redondance et de son application à l'amélioration du niveau de sécurité des systèmes à microprocesseur.

Lorsque de tels systèmes sont utilisés en tant que circuits de commande de machines, ils doivent respecter l'article R 233-97, du code du travail : « Prévention des effets dangereux des défaillances du système d'alimentation en énergie et du circuit de commande », [4] à savoir :

« Une défaillance, une panne ou une détérioration du système d'alimentation en énergie ou du circuit de commande des machines et appareils ne doit :
– ni provoquer la mise en marche intempestive d'un élément mobile de la machine,
– ni rendre inefficace les dispositifs de protection des éléments mobiles », ce que nous résumerons par le fait que le système doit être conçu en sécurité positive.

Le présent document est un recensement des différentes formes de redondance rencontrées dans les systèmes à microprocesseur. Il constitue une synthèse bibliographique réalisée de façon préliminaire à un travail de doctorat effectué au Service Électronique-Sécurité des Systèmes de l'I.N.R.S. à Vandœuvre.

Le lecteur pourra trouver dans cet article :
– un ensemble de définitions et d'architectures de systèmes redondants,
– une étude sur l'application du concept de redondance :
• au niveau des organes de traitement qu'ils soient matériels ou/et logiciels;

→

*Figure 3 :* Architectures de systèmes utilisant la redondance à des fins de sécurité et/ou disponibilité (suite).
*System architectures which use redundancy for safety and/or availability (continued).*

| Architecture | Désignation | Spécification | Référence |
|---|---|---|---|
| E, e1, Superviseur, e2, S | Redondance sélective active<br><br>e1 = e2 : homogène<br>e1 ≠ e2 : hétérogène | Les unités e1 et e2 assurent toutes deux la réalisation de la mission; un superviseur effectue la comparaison des résultats de traitement :<br>– seuls les résultats de e1 sont validés en sortie du système en cas de convergence,<br>– en cas de divergence, le superviseur localise l'unité défaillante à l'aide d'un programme-test et effectue le basculement du commutateur selon le résultat obtenu.<br>Ce type d'architecture est utilisé pour assurer la disponibilité d'un système. | 4 |
| E, e1, Superviseur, e2, S | Redondance sélective passive<br><br>e1 = e2 : homogène<br>e1 ≠ e2 : hétérogène | – Tiède :<br>l'unité e1 assure seule la réalisation de la mission, l'unité e2 est utilisée pour réaliser des tâches secondaires; ce n'est qu'après défaillance de e1 que e2 sera utilisée pour assurer la mission requise, les données nécessaires à la reprise sont mémorisées à intervalles réguliers à l'intérieur de mémoires de e2 par l'intermédiaire du superviseur.<br>Ce type d'architecture est utilisé pour assurer la disponibilité d'un système. | 5 |
| | | – Froide :<br>l'unité e1 assure seule la réalisation de la mission, l'unité e2 est inactive ou totalement déconnectée.<br>Ce n'est qu'après défaillance de e1 que e2, après une initialisation complète, assurera la réalisation de la mission.<br>Ce type d'architecture est utilisé pour assurer la disponibilité d'un système. | 6 |

• au niveau des informations, lors des phases acquisition et traitement.

## Généralités et définitions

### A propos du mot « redondance »

Le Larousse Etymologique [5] donne pour le mot « redondance » : XIV$^{e}$ siècle, du latin redundantia, de redundare « même évolution de sens ».

L'origine latine du mot redondance est explicitée dans [6] : redundantia : trop plein, débordement, excès, redondance (de style).

Ces deux définitions se résument par le fait que la redondance est un excès dans un discours ou une émission de signal, avec une même évolution de sens.

Si la redondance verbale a pour but de renforcer la compréhension ou d'enjoliver un message, la redondance utilisée en électronique est là pour améliorer la sécurité (et/ou la disponibilité), sans pour autant ajouter quelque chose au fonctionnement de base. C'est ce que traduit la définition de ce mot dans la norme NF Z 61-000 [1] : « multiplications de certains composants, sous-systèmes, systèmes dans le but d'assurer une mission donnée en présence de défaillances ».

Dans la suite de ce document, certaines architectures décrites sont utilisées pour assurer la disponibilité d'un dispositif : elles correspondent à des systèmes dits « à tolérance aux fautes ». Notre préoccupation étant principalement la sécurité des systèmes, nous ne les développerons pas davantage.

## *Différentes formes de redondances [7]*

Nous distinguerons deux catégories selon que la redondance s'applique à l'organe de traitement, ou à l'information traitée.

Auparavant, nous donnerons les définitions suivantes :
- **unité ou chaîne primaire :** partie ou ensemble d'un système qui est reproduit à un ordre n déterminé et qui, à lui seul, est capable d'effectuer la mission requise;
- **unité ou chaîne redondante :** reproduction de l'unité primaire;
- **degré ou ordre d'une redondance :** correspond au nombre de n-plications effectuées sur le système considéré;
- **tâche :** succession de séquences d'instructions;
- **mission :** succession de tâches.

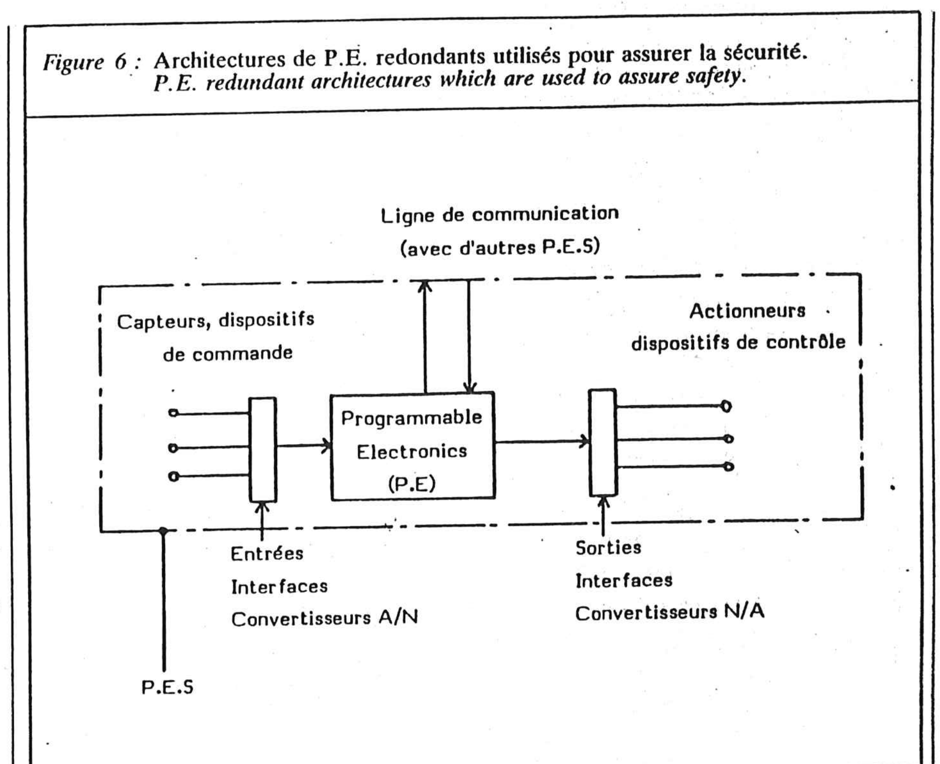



*Figure 6 :* Architectures de P.E. redondants utilisés pour assurer la sécurité.
*P.E. redundant architectures which are used to assure safety.*

### • Redondance de l'organe de traitement

*nature de la redondance*
- **massive :** l'unité (ou les unités) redondante(s) effectue(nt) la mission au même titre que l'unité primaire, le processus étant piloté par l'ensemble des sorties des différentes chaînes, soit directement, soit à travers un organe de contrôle qui peut prendre l'une des deux formes suivantes :
  - . comparateur : toute divergence des résultats de sortie de chacune des chaînes entraîne l'arrêt ou la mise en sécurité du processus. Ce type de contrôle est utilisé pour assurer la sécurité d'un système;
  - . voteur : suivant le nombre d'unités constituant le système et selon le critère de vote choisi (par exemple, deux réponses bonnes parmi trois (2/3), trois parmi quatre (3/4),...), un certain nombre de divergences au niveau des résultats de sortie de chacune des chaînes peuvent être masquées. Ce type de contrôle est utilisé pour assurer la sécurité et la disponibilité d'un système.
- **Sélective :** seules les sorties de l'unité primaire commandent le processus. En cas de défaillance de celle-ci, c'est la ou l'une des unités redondantes qui assurera la continuité de la mission. Il existe donc un organe de décision qui détecte les défaillances et assure ou demande la commutation d'une unité de secours sur le processus.

Selon la nature du fonctionnement de l'unité redondante, on distingue deux cas de redondance sélective :
- . la redondance sélective active (appelée aussi redondance dynamique) pour laquelle l'ensemble des unités effectue les mêmes traitements, l'unité (ou les unités) redondante(s) étant toujours en attente pour remplacer l'unité primaire en cas de défaillance de celle-ci;
- . la redondance sélective passive (appelée aussi redondance statique) pour laquelle l'unité (ou les

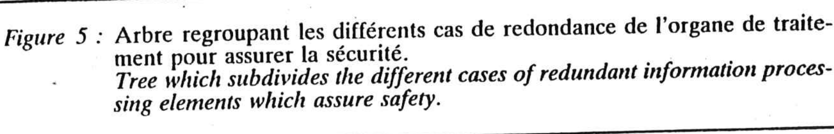


*Figure 5 :* Arbre regroupant les différents cas de redondance de l'organe de traitement pour assurer la sécurité.
*Tree which subdivides the different cases of redundant information processing elements which assure safety.*

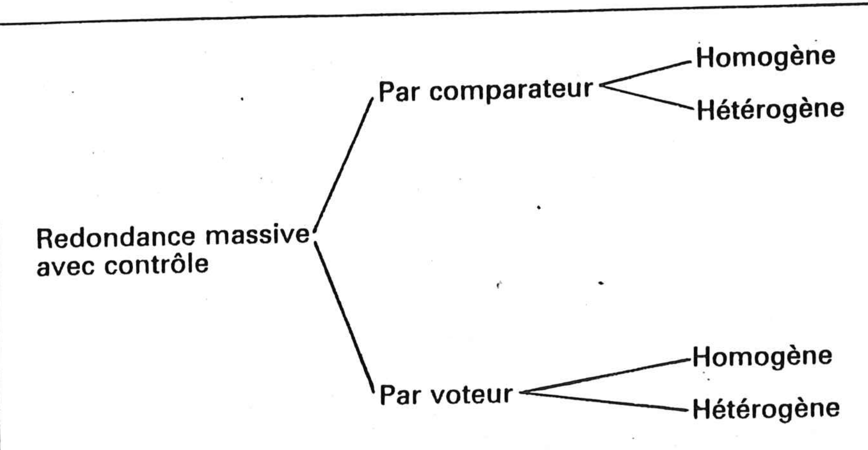


*Figure 4 :* Diagramme illustrant les termes P.E. et P.E.S.
*Diagram of P.E. and P.E.S. terms.*

| Architecture | Désignation | Spécification | Référence |
|---|---|---|---|
| P.E (L1, M1) ; P.E (L1, M1) → Comparateur → S | Redondance matérielle globale homogène d'ordre 2 | Les deux P.E. effectuent la même mission; le comparateur effectue le contrôle de coïncidence des résultats fournis par chacune des P.E. : toute divergence entraîne la mise en sécurité du système. Le comparateur doit être en sécurité intrinsèque, capable de détecter ses propres défauts. | 1 |
| P.E (L1, M1) ; P.E (L2, M2) → Comparateur → S | Redondance matérielle globale hétérogène d'ordre 2. | Identique à référence 1. Les deux chaînes sont dans ce cas différentes tant au niveau matériel que logiciel (M1 ≠ M2 et L1 ≠ L2). | 2 |
| P.E (L1, M1) ; P.E (L2, M1) → Comparateur → S | Redondance matérielle globale hétérogène d'ordre 2. | Identique à référence 1. L'hétérogénéité se situe ici seulement au niveau logiciel (L1 ≠ L2). | 3 |

unités) redondante(s) effectue(nt) des missions différentes de celle réalisée par l'unité primaire (généralement des tâches secondaires); la défaillance de l'unité primaire entraîne la communication sur l'une des unités redondantes :
- si les unités en attente disposent des informations pour assurer directement la reprise en main du système lors d'une défaillance de l'unité primaire, on parlera de redondance sélective passive tiède;
- si une initialisation totale, automatique ou manuelle (unité en attente inactive ou non alimentée) est nécessaire à la reprise par l'unité en attente, on parlera de redondance sélective passive froide.

La redondance sélective est utilisée pour assurer la disponibilité d'un système.

*type de la redondance*
- **globale :** elle correspond à la duplication (n-plication) de l'ensemble du système;
- **locale :** elle correspond à la duplication (n-plication) d'une partie du système.

*niveau d'application de la redondance*
- **matérielle :** elle correspond à la duplication (n-plication) du matériel ou d'une partie du matériel constituant le système;
- **logicielle :** elle correspond à la duplication (n-plication) du logiciel ou d'une partie du logicel d'un système à une seule chaîne.

*mise en œuvre de la redondance*
- **homogène :** les parties redondantes et primaire sont totalement identiques et ce, au niveau matériel et logiciel;
- **hétérogène :** les parties redondantes et primaire sont différentes et ce au niveau matériel et/ou logiciel. Selon le cas, le degré d'hétérogénéité sera plus ou moins important suivant que l'on utilisera une logique, une architecture ou une technologie différente (cf. chapitre « redondance matérielle »).

Les différentes possibilités de redondance énoncées précédemment sont illustrées par la figure 1.

*Figure 7 :* Architectures de P.E. redondants utilisés pour assurer la sécurité (suite).
*P.E. redundant architectures which are used to assure safety (continued).*

| Architecture | Désignation | Spécification | Référence |
|---|---|---|---|
| P.E (1) / P.E (i) / P.E (n) → Voteur → S<br>Voteur de type p parmi n avec $p > n/2$ | Redondance matérielle globale d'ordre n<br>– homogène si P.E. (i) = P.E. (j) $i = 1 \ldots n, i \neq j$<br>– hétérogène si P.E. (i) ≠ P.E. (j) $i = 1 \ldots n, i \neq j$ | Les n P.E. effectuent la même mission. Un voteur à sécurité intrinsèque effectue le contrôle des différentes sorties. Il fournit une sortie relative à p résultats identiques parmi n possibles : si plus de (n-p) résultats de sortie divergent, le système est mis dans un état de sécurité. | 4 |
| E / P.E / L / M1 / M11 / M12 / C<br>Suite du traitement<br>Mise en sécurité | Redondance matérielle locale d'ordre 2 :<br>– homogène si M 11 = M 12<br>– hétérogène si M 11 ≠ M 12 | L'élément redondant matériel effectue la mission au même titre que l'élément primaire. Un comparateur vérifie la coïncidence des résultats de sortie et déclenche une mise en sécurité en cas de divergence.<br>Remarque : il est possible pour un ordre supérieur à 2 d'utiliser un voteur : la redondance matérielle locale sera dans ce cas de type :<br>– C si M 11 = M 12 = M 13 = .....<br>– D si M 11 ≠ M 12 ≠ M 13 ≠ ..... | 5 |
| E / P.E / M / L11 / L11 / L12 / C<br>Suite du traitement<br>Mise en sécurité | Redondance logicielle locale d'ordre 2 :<br>– homogène si L 11 = L 12<br>– hétérogène si L 11 ≠ L 12 | L'élément redondant logiciel effectue la mission au même titre que l'élément primaire. Un comparateur vérifie la coïncidence des résultats de sortie et déclenche une mise en sécurité en cas de divergence.<br>Remarque : il est possible pour un ordre supérieur à 2 d'utiliser un voteur : la redondance logicielle locale sera dans ce cas de type :<br>– C si L 11 = L 12 = L 13 = .....<br>– D si L 11 ≠ L 12 ≠ L 13 ≠ ..... | 6 |

- **Redondance de l'informatique traitée**

La redondance d'informations correspond à l'adjonction à un mot d'informations, de bits supplémentaires dans le but d'en assurer le contrôle.

- **Redondance hybride**

Elle correspond à une combinaison des différentes formes de redondances citées précédemment et cela sur un même système.

| | Référence |
|---|---|
| • Redondance massive :<br>– sans contrôle<br>– avec contrôle : – par comparateur<br>– par voteur | 1<br>2<br>3 |
| • Redondance sélective :<br>– active<br>– passive : – tiède<br>– froide | 4<br>5<br>6 |

Les figures 2 et 3 illustrent les références 1 à 6 citées ci-dessus.

### *Architectures des systèmes utilisant la redondance à des fins de sécurité et/ou de disponibilité*

Les architectures décrites s'appliquent pour des redondances de type matériel ou logiciel, qu'elles soient globales ou locales.

### *Architectures d'électroniques programmables redondantes utilisées pour assurer la sécurité [8]*

Dans ce paragraphe et dans la suite de ce document, nous nous intéressons uniquement aux Electroniques Programmables, chez les Anglo-Saxons « Programmable Electronics » (P.E.) : cette terminologie est celle utilisée par un groupe de travail de la Communauté Européenne regroupant sept organismes de quatre pays différents (R.F.A., Grande-Bretagne, Danemark et France) et auquel participe l'I.N.R.S.

Avant de détailler les architectures de ces électroniques programmables, il est bon de préciser la différence entre les deux abréviations :
– P.E.S. : Système Electronique Programmable;
– P.E. : Electronique Programmable.

La figure 4 illustre les deux termes P.E. et P.E.S. [9].

Seules les architectures de P.E. utilisées pour assurer la sécurité seront considérées : les références 2 et 3 du paragraphe III seront donc les seules développées.

La redondance massive sans contrôle, homogène ou hétérogène est utilisée en général de façon locale, soit au niveau de composants (doublage des relais de sortie par exemple), soit au niveau de sous-ensembles (alimentation secourue...); cette redondance n'étant pas spécifique aux P.E., nous ne la développerons pas davantage.

Pour l'application à la sécurité des systèmes électronique, l'arbre de la figure 1 se réduit à la figure 5, représentée page 48.

Cette redondance massive avec contrôle s'applique à du matériel ou du logiciel, elle peut être globale ou locale.

Les figures 6 et 7 illustrent les architectures de P.E. redondantes, utilisant la redondance massive avec contrôle.

Les abréviations L et M utilisées se rapportent respectivement à Logiciel et Matériel.



### *Références bibliographiques*

[1] NF Z 61-000 « Vocabulaire international de l'informatique ».
[2] NF X 06-501 « Introduction à la fiabilité ».
[3] MIL STD 882 « Requirements for system safety programm for systems and associated systems and equipments ».
[4] « Intégration de la sécurité dans la conception des machines et appareils : réglementation générale, textes et commentaires ». Ministère du Travail - I.N.R.S., avril 1983.
[5] A. Dauzat, J. Dubois, H. Mitterand. – « Larousse Étymologique ». Librairie Larousse, 1971.
[6] H. Goelzer. – « Le Latin en poche ». Dictionnaire Latin/Français. Garnier, Paris, 1928.
[7] J.-C. Laprie. – « Architecture et évaluation des systèmes informatiques sûrs de fonctionnement ». Note technique LAAS-ASF 81.T.14, avril 1984.
[8] « Assessment, architecture and performance of industrial programmable electronic systems with particular reference to robotic safety ». C.E.C. Collaborative Project. Objective 5 : Interium Report n° 2.
[9] « Guidance on the safe use of programmable electronic systems :
. Part. 1 : General requirements;
. Part. 2 : Safety integrity assessment.
Health and Safety Executive, october 1984.

# Amélioration du niveau de sécurité des systèmes à microprocesseur par application du concept de redondance

## 2e partie

**Les différents cas de redondance sont développés dans cette partie : nous nous limitons à l'étude des architectures de systèmes devant fonctionner en sécurité positive. Les redondances matérielle, logicielle et d'information sont décrites afin d'aiguiller concepteurs et utilisateurs sur le choix de formes de redondance à utiliser selon les contraintes de mise au point, coût, maintenance et selon le niveau de sécurité recherché.**

**B. Kopka et J.P. Gérardin**

INKS, Centre de Recherche
Département « Ergonomie-Sécurité »
Section « Électronique-Sécurité de Systèmes »
BP 27, 54501 Vandœuvre Cedex.

**Improving the safety level of programmable electronic systems by application of the concept of redundancy**

*The different cases of redundancy are developed in this part: we will limit this article to a review of system architectures which must have fail safe operation. Hardware, software and information redundancies are described to guide designers and users in making choices as to which form of redundancy to use within the constraints of development, cost, and maintenance and according to the safety level desired.*

## Redondance de l'organe de traitement

Dans ce chapitre, nous allons étudier quelques-unes des méthodes de mise en œuvre du principe de redondance couramment utilisées dans les systèmes à microprocesseur en essayant de préciser les avantages et les inconvénients de chacune d'entre elles et en analysant le niveau de sécurité qu'elles procurent.

### Redondance matérielle

- **Redondance locale** [1]

Nous considérons la redondance matérielle locale sur une chaîne unique : elle correspond à la duplication ou n-plication d'éléments vitaux dont la défaillance pourrait entraîner une situation dangereuse. Le choix des sous-ensembles devant être dupliqués sera laissé au concepteur du système qui, à partir du cahier des charges, de la no- →

menclature des éléments utilisés et de leurs caractéristiques, établira la liste des éléments ou groupe d'éléments susceptibles d'entraîner des situations dangereuses après défaillance.

Ce pourrait être, par exemple, la duplication du microprocesseur et de ses entrées, selon le schéma de la figure 8.

- **Redondance globale** [1], [2], [3]

Nous considérons le cas de systèmes électroniques totalement dupliqués ou n-pliqués possédant comme organe de contrôle de coïncidence un comparateur ou un voteur.

*Homogène*

- Chaînes synchronisées [4]

L'acquisition des données, le traitement de l'information et la libération des valeurs de sorties vers l'organe de contrôle sont totalement synchrones. La figure 9 illustre le déroulement temporel de trois chaînes synchronisées.

T0 = T'0 = T''0; T1 = T'1 = T''1;
T2 = T'2 = T''2; T3 = T'3 = T''3

Une comparaison permanente doit être effectuée au niveau des informations délivrées en sortie : l'organe de contrôle de coïncidence (comparateur ou voteur) doit détecter toute divergence de résultats sur l'ensemble des chaînes.

L'utilisation de chaînes identiques synchronisées ne met pas le système à l'abri des défaillances de mode commun; en effet, une perturbation (microcoupure, surtension, parasite conduit ou rayonné...) peut altérer le système au moment de la lecture des données, au cours du traitement ou à la libération des valeurs de sorties : chaque système délivre alors, vers l'organe de contrôle de coïncidence, la même valeur erronée. Ce dernier est alors incapable de déceler la défaillance.

Pour remédier à cet inconvénient, on peut utiliser des chaînes identiques quasi synchronisées.

- Chaînes quasi synchronisées [2]; [4]

L'acquisition des données, le traitement de l'information et la libération des valeurs de sorties vers l'organe de contrôle sont décalés dans le temps : quelques périodes d'horloge séparent chacun des débuts de cycles de l'ensemble des chaînes de façon à ce que la même instruction ne soit jamais effectuée au même instant dans deux chaînes différentes.

La figure 10 illustre le déroulement temporel de trois chaînes quasi synchronisées.

$$T''i = T'i + \Delta T; \quad T'i = Ti + \Delta T$$

Le dispositif de contrôle de coïncidence acquiert les valeurs de sortie une à une et délivre une valeur de sortie finale après la lecture des résultats de la dernière chaîne. Le processus évoluant avec des chaînes dont le fonctionnement est décalé dans le temps, tout parasitage affectant le système produira des effets différents d'une chaîne par rapport aux autres : il y aura discordance et, par conséquent, détection par le système de coïncidence.

Toutefois, des problèmes nouveaux sont engendrés par l'utilisation de cette méthode : une modification des données peut intervenir dans le laps de temps séparant les lectures effectuées par chacune des voies; le dispositif de coïncidence ne peut pas faire la différence entre panne sur une chaîne et désaccord passager : ce conflit est appelé « divergence » et peut être résolu par l'établissement d'un dialogue entre chaînes. Ces dernières, au cours des phases d'acquisition des entrées, comparent mutuellement leurs données et procèdent à une nouvelle lecture tant qu'il n'y a pas identité parfaite entre toutes les valeurs lues : ce type de dialogue est appelé « antidivergence ».

La figure 11 illustre l'architecture d'un système redondant composé de deux chaînes identiques.

*Hétérogène* [4], [5]

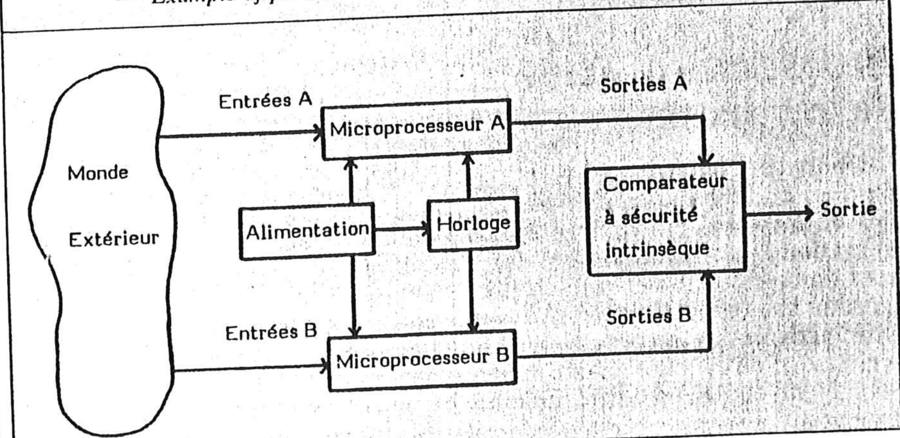
Chaque chaîne est physiquement différente : par son principe, la redondance hétérogène permet de supprimer la plupart des défauts de mode commun. En effet, chacune des chaînes constituant le système aura en principe une réaction différente lors de l'apparition de perturbations.

- Techniques différentes

La méthode la plus radicale et la plus extrême pour éliminer les défauts de mode commun correspond à l'utilisation, pour chacune des chaînes du dispositif, de techniques différentes : pneumatique, hydraulique, à relais ou électronique classique, le concepteur peut diversifier chacune des chaînes de façon à obtenir une redondance à fort niveau d'hétérogénéité.

Un exemple possible est celui de la figure 12 où l'on trouve un système constitué d'une carte à microprocesseur dupliquée par une logique électromécanique.

Figure 8 — Exemple d'une redondance locale d'ordre deux.
— *Example of partial redundancy with two channels.*



L'utilisation d'une telle méthode assure à un système un niveau de sécurité très élevé; cette solution reste envisageable malgré les problèmes qui lui sont associés :

– calculs de fonctions complexes impossibles à réaliser avec certaines techniques,
– problème de différence de temps de réponse entre les chaînes,
– nécessité de mettre en œuvre des interfaces d'entrées et de sorties pour assurer la compatibilité des signaux à traiter d'une part et à comparer d'autre part au niveau du dispositif de contrôle de coïncidence,
– encombrement matériel important de certaines techniques par rapport à l'utilisation de chaînes électroniques à circuits intégrés (LSI, VLSI, ...).

De plus, cette complexité de mise en œuvre aura d'importantes répercussions sur le coût final du système, sa durée de mise au point et sa facilité de maintenance.

• Technologies différentes

La technologie apparaît comme étant une classe d'une technique donnée. Plus utilisée par les professionnels de la sécurité, la redondance utilisant des technologies différentes présente moins d'inconvénients que l'utilisation de techniques différentes.

L'exemple de la figure 13 illustre un système, utilisant la technique électronique, constitué de deux chaînes construites autour de microprocesseurs de technologies différentes.

Grâce à des facteurs d'immunité aux bruits différents selon la technologie, le comportement de chaque chaîne est différent lors de l'apparition de parasites : la discordance est détectable par le système de coïncidence. Des problèmes subsistent au niveau de la vitesse d'exécution, du synchronisme et de la compatibilité technologique.

• Architectures différentes

La redondance hétérogène basée sur des architectures différentes correspond à l'utilisation, pour chaque chaîne, de cartes électroniques standard, et organisées de manières différentes.

Cette méthode est illustrée par la figure 14 où l'on trouve un système constitué de trois chaînes en technique électronique et réparti comme suit :

– chaîne n° 1 : carte microprocesseur, fabricant X,
– chaîne n° 2 : carte microprocesseur, fabricant Y,
– chaîne n° 3 : carte microprocesseur, fabricant Z.

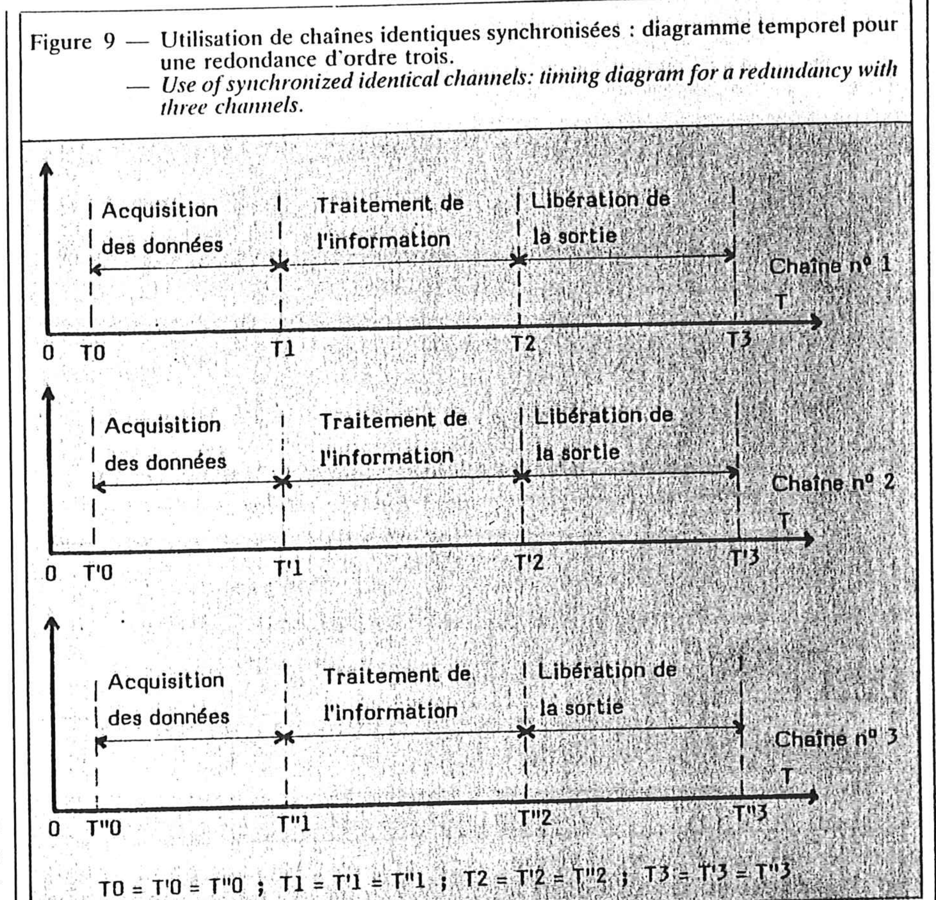



Figure 9 — Utilisation de chaînes identiques synchronisées : diagramme temporel pour une redondance d'ordre trois.
— *Use of synchronized identical channels: timing diagram for a redundancy with three channels.*

Cette méthode peut parfois être couplée avec celle concernant l'utilisation de technologies différentes, architecture et composants étant différents.

• Logiciels différents [6], [7]

Des logiciels différents sont utilisés pour chacune des chaînes : la redondance est hétérogène au niveau du logiciel. L'acquisition des valeurs d'entrées peut s'effectuer de manière synchronisée ou quasi-synchronisée, la deuxième solution devant permettre l'élimination des défauts de parasitage lorsque l'entrée est commune à toutes les chaînes.

Les logiciels constituant chacune des chaînes doivent être conçus, vérifiés par des équipes « logicielles » différentes et élaborés à partir du même cahier des charges.

Outre la difficulté et la complexité de la mise en œuvre, quelques problèmes sont liés à cette méthode :

– le temps total de mise au point est important pour ce type de réalisation,
– le coût total est d'autant plus élevé que le nombre de chaînes constituant le système est important.

Dans cette partie, le lecteur a été sensibilisé aux différentes formes de redondance matérielle.

L'hétérogénéité semble théoriquement être la méthode qui procure le niveau de sécurité le plus élevé. Tout concepteur désirant élaborer un système à microprocesseur de sécurité devra, lors du choix de la forme de redondance à utiliser, faire la part des choses →

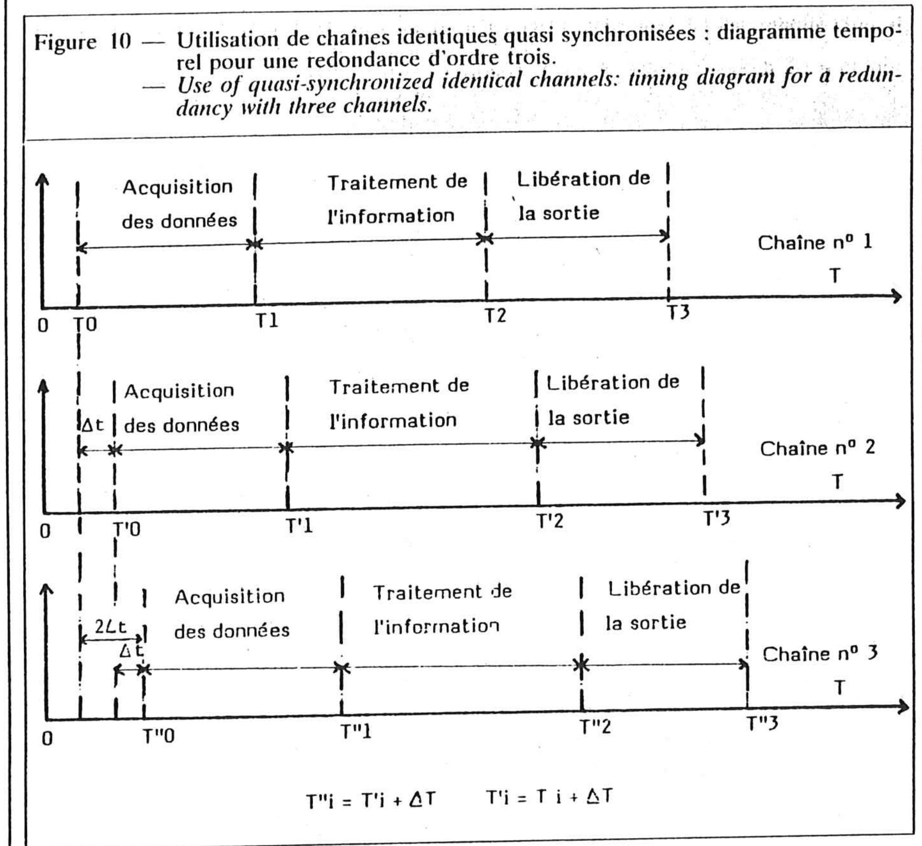



Figure 10 — Utilisation de chaînes identiques quasi synchronisées : diagramme temporel pour une redondance d'ordre trois.
— *Use of quasi-synchronized identical channels: timing diagram for a redundancy with three channels.*

entre le niveau de sécurité recherché d'une part et, d'autre part, les différentes contraintes mentionnées pour chacune des méthodes présentées ici.

## • Références bibliographiques

[1] A. Schweitzer, J.P. Gérardin. — « Méthodes permettant d'améliorer le niveau de sécurité des systèmes à logique programmée ». Revue « E.T.I. », n° 12, novembre 1984 et n° 13, décembre 1984.

[2] H. Holscher, J. Rader. — « Microcomputer in safety techniques : an aid to orientation / problem solving for developer and manufacturer ». TÜV Rheinland, october 1984.

[3] K.A. Wobig. — « Fail safe microcomputer systems for railway signaling. Problems and possibilities ». Siemens AG, Braunschweig, Germany.

[4] K.B. Klaassen, J.C.L. van Peppen. — « Hazard of inhomogeneous redundant systems with imperfect sensing and switching ». Reliability in electrical and electronic components and systems. F. Lauger and J. Moltoft (Editors). North – Holland Publishing Company 1982.

[5] J. Arlat. — « Conception d'un microcalculateur tolérant aux fautes par diversification fonctionnelle ». Thèse de Docteur Ingénieur de l'Institut National Polytechnique de Toulouse, avril 1979.

[6] R. Habicht, E. Knoernschild, M. Popp, J. Rader. — « Requirements, safety measures and test procedures for the hardware safety of microcomputer systems for use in technical safety applications ». TU e.V, Bayern e.V, München.

[7] M.L. Shooman. — « Software engineering: design, reliability and management ». Mc Graw-Hill Book Company, 1983.

## *Redondance logicielle* [1], [2]

Cette forme de redondance, plus communément appelée « redondance temporelle », consiste à faire exécuter séquentiellement la même fonction par des modules de programmes identiques ou différents.

Les parties de logiciel ajoutées dans des buts de contrôles, tests ou aides à diagnostic ne constituent pas, à proprement parler, une redondance logicielle.

### • Différentes formes de redondance logicielle [3], [4]

*Une seule version répétée dans le temps*

Cette méthode consiste à écrire le programme de telle sorte qu'une tâche ne soit considérée comme terminée que si une même séquence d'instructions a été répétée une ou plusieurs fois dans le temps, cette dernière n'étant présente qu'une fois en mémoire.

A l'issue de chacune de ces séquences, les résultats sont stockés à des emplacements mémoires différents. Au $n^{ième}$ résultat fourni, le contrôle s'effectue par une comparaison logicielle délivrant un résultat unique en sortie; toute discordance des résultats entraîne une mise en sécurité du système.

La séquence d'instructions ainsi considérée doit être exempte de toute erreur de conception afin d'éviter la répétition de traitements erronés qui fourniraient des résultats identiques en sortie bien que totalement faux. D'autre part, il faut prêter une attention particulière à la programmation de la tâche d'acquisition de données.

*n versions*

Une variante du cas précédent consiste à exécuter successivement des tâches assurant la même fonction par des séquences d'instructions stockées à des emplacements mémoires différents.

Dans le but d'effectuer une répartition spatiale et afin d'éviter le parasitage simultané de l'ensemble des n versions, il sera bon d'utiliser des boîtiers mémoires différents. Ces n versions peuvent être homogènes ou hétérogènes.

*Caractéristiques de ces méthodes*

Ces méthodes peuvent être appliquées lors de la conception d'un système ou lors de sa phase

d'exploitation (par exemple : programme d'application d'un automate programmable...). Dans ce dernier cas, le temps d'exécution est pénalisé et peut être néfaste pour des applications en « temps réel ».

Les avantages et les inconvénients de ces méthodes sont les suivantes :

— avec l'utilisation d'une seule version :
- détection de défauts fugitifs sur mémoires RAM ou bus interne,
- un seul emplacement mémoire utilisé pour le stockage de la version.

— avec l'utilisation de n versions homogènes :
- détection de défauts fugitifs ou permanents sur certains emplacements mémoires (collage de bits...),
- utilisation d'une seule équipe de conception/programmation,
- mise au point identique à l'utilisation d'une seule version,
- taille mémoire pouvant se révéler importante.

— avec l'utilisation de n versions hétérogènes :
- détection de défauts fugitifs et permanents,
- détection de défaillances internes du microprocesseur,
- détection d'erreurs de programmation,
- taille mémoire parfois importante,
- utilisation de plusieurs équipes de conception/programmation avec diversification des outils d'analyse,
- temps total de l'étude important,
- coût total élevé,
- mise au point plus complexe.

Les trois configurations citées ci-dessus montrent que l'on peut améliorer le niveau de sécurité d'un système en utilisant la redondance logicielle; la première propose une solution réalisable a posteriori sur le système, l'utilisation des n versions nécessite par contre des modifications des cartes électroniques notamment au niveau des plans mémoires. Ces derniers répartis spatialement auront une réaction différente aux parasites et la défaillance de l'un d'eux ne pénalisera pas l'ensemble du système.

- **Références bibliographiques**

[1] A. Schweitzer, J.P. Gérardin. — « Méthodes permettant d'améliorer le niveau de sécurité des systèmes à logique programmée ». Revue « E.T.I. », n° 12, novembre 1984 et n° 13, décembre 1984.

[2] K.D. Heidtman. — « Time redundancy with applications to electronical devices ». Reliability in electrical and electronic components and systems. E. Lauger and J. Moltoff (Editors). North – Holland Publishing Company, 1982.

[3] H. Holscher, J. Rader. — « Microcomputer in safety techniques : an aid to orientation/problem solving for developer and manufacturer ». TUV Rheinland, october 1984.

[4] O. Andersen, P.G. Petersen. — « Standards and regulation for software approval and certification ». Electronik Centralen, june 1984.

## Redondance d'informations

On peut, sur un système, faire la distinction entre deux types d'informations :

— Les informations venant du monde extérieur,

— Les informations en cours de traitement par l'unité centrale.

Afin d'assurer l'intégrité de la sécurité du système, différentes méthodes peuvent être utilisées.

### Informations venant du monde extérieur

Que ce soit pour un système simple (une chaîne) ou pour un système complexe (deux chaînes ou plus), l'acquisition des données du monde extérieur par ledit système est un problème d'importance primordiale; quelques précautions élémentaires sont à respecter :

— on veillera à utiliser autant de capteurs d'entrées que de nombre de chaînes utilisées,

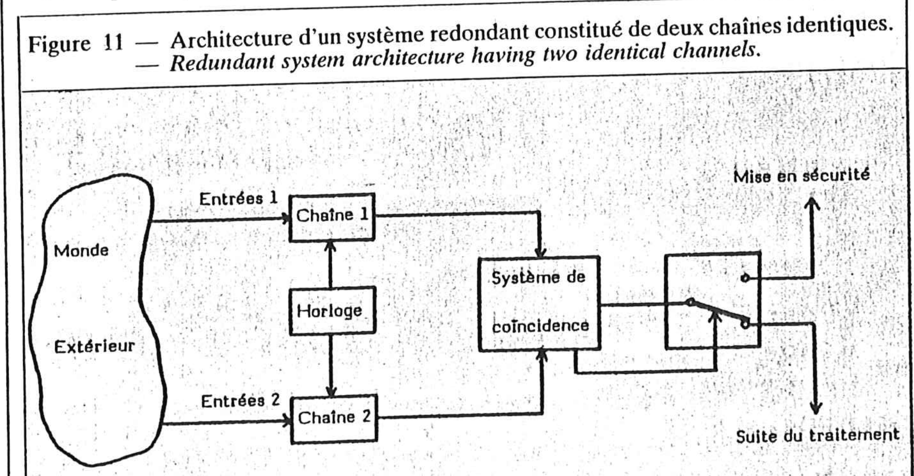
— on diversifiera, si possible, ces dispositifs d'acquisition d'une chaîne par rapport aux autres de façon à éviter les défauts de mode commun,

— on établira après chaque lecture et chaque fois que possible une procédure de dialogue entre toutes les chaînes afin de vérifier la cohérence et l'identité des valeurs à traiter,

— les précisions des dispositifs d'acquisition analogique pouvant varier d'une chaîne à l'autre, on établira un écart admissible entre chacune des valeurs lues par les différents capteurs utilisés.

Pour les capteurs de type « tout ou rien », on utilisera des capteurs à sécurité intrinsèque (par exemple, des contacteurs à contacts à arrachement). Avec les capteurs analo-

Figure 11 — Architecture d'un système redondant constitué de deux chaînes identiques.
— *Redundant system architecture having two identical channels.*



giques, on effectuera un contrôle de vraisemblance (identité des valeurs lues avec les valeurs prédites, appartenance de la valeur lue à une plage de valeurs déterminées...).

## Informations en cours de traitement par le système

Nous nous limiterons ici à quelques définitions succinctes des types de redondance appliqués à ce genre d'informations et nous mentionnerons les principaux codes utilisés.

### • Mise en œuvre de la redondance [1], [2]

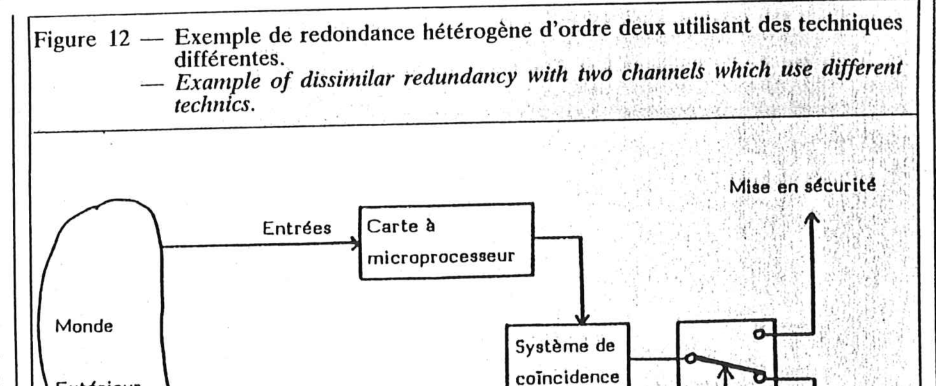
A la suite de parasitage (bruit, rayonnement, microcoupure, surtension), des informations utiles, bits ou mots, peuvent être altérées : il est donc impératif de mettre en œuvre des moyens de contrôle de la validité de ces informations et notamment d'avoir recours à la redondance.

Cette dernière sera utilisée dans les transferts de données, parallèles ou séries, entre les organes d'entrée, de traitement, de stockage et de sortie.

Elle correspond soit à un codage d'un mot de données, soit à une adjonction à ce mot, de bits supplémentaires. Dans le premier cas, il s'agit d'une structure dite d'informations non séparables, dans le second cas d'une structure d'informations séparables.

Dans les deux cas, la mise en œuvre nécessite du matériel et (ou) du logiciel supplémentaire.

Figure 12 — Exemple de redondance hétérogène d'ordre deux utilisant des techniques différentes.
— *Example of dissimilar redundancy with two channels which use different technics.*




### • Informations séparables

L'information utile est totalement incluse, sans déformation dans le message codé, ce dernier étant obtenu par adjonction aux bits de l'information utile, de bits supplémentaires (parfois appelés « clés de contrôle »).

Nous citerons pour mémoire les codes séparables les plus connus ainsi que des références bibliographiques :

— bit de parité ou contrôle par redondance verticale : [1], [4], [5]
— contrôle par redondance horizontale : [1], [5]
— code linéaire entrelacé : [4], [6]
— contrôle par redondance cyclique : [1], [4], [7]
— checksum : [4], [8]
— code de Hamming et code de Hamming « modifié » : [9], [10], [11]
— code résidu A : [4]
— code de Berger : [12], [2]

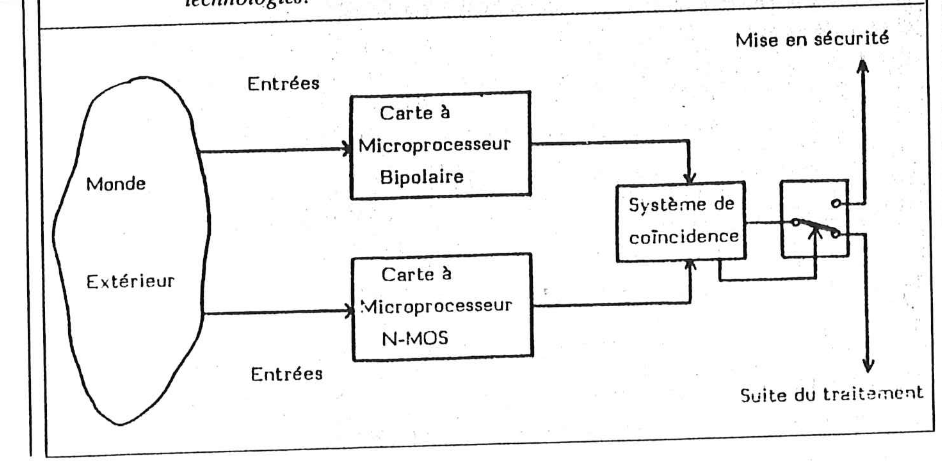
### • Informations non séparables [3]

Elles sont obtenues par un codage de l'information utile grâce à des tables de conversion ou un ensemble d'opérations logiques appliqué au mot traité.

Nous mentionnons ci-dessous les codes non séparables les plus connus :

— code arithmétique AN : [4], [7]
— code « k parmi n » et code « double rail » : [3], [4]

Figure 13 — Exemple de redondance hétérogène d'ordre deux utilisant des technologies différentes.
— *Example of dissimilar redundancy with two channels which use different technologies.*




### • Références bibliographiques

[1] Nghiem Phong Tuan. — « Transmission des données ». Éditions Infoprax, 1979.
[2] D.A. Anderson. — « Design of self checking digital networks using coding techniques ». Departement of Electrical Engineering, University of Illinois, september 1971.

[3] J.C. Geffroy. — « Test en ligne et sécurité des systèmes logiques ». Thèse d'État, Université Paul-Sabatier, Toulouse, 1976.
[4] G. Saucier, C. Bellon. — « La tolérance aux pannes dans les systèmes à microprocesseurs ». Rapport IMAG.
[5] J.P. Auclair, J.M. Wiss. — Colloque « Systèmes électroniques sûrs ». Informatique et Signalisation, Direction de l'équipement SNCF, septembre 1980.
[6] G. Coiffet. — « Théorie et techniques de la transmission des données ». Masson, 1977.
[7] G. Cullmann. — « Codes détecteurs et correcteurs d'erreurs ». Dunod, Paris, 1967.
[8] H. Holscher, J. Rader. — « Microcomputers in safety techniques : an aid to orientation/problem solving for developer and manufacturer ». TUV Rheinland, 1984.
[9] R.W. Hamming. — « Error detecting and error correcting codes ». The Bell System Technical Journal, april 1950.
[10] M. Baconnier. — « Détection et correction des erreurs de mémoires : les principes fondamentaux ». Revue « Minis et Micros », n° 160, mars 1982.
[11] C. Gaschet. — « Le circuit détecteur et correcteur d'erreurs simples et doubles ». Revue « Électronique Industrielle », n° 20, septembre 1981.
[12] J.M. Berger. — « A note on error detection codes for asymmetric channels ». Information and Control, march 1961.

Figure 14 — Exemple de redondance hétérogène d'ordre trois utilisant des architectures différentes.
— *Example of dissimilar redundancy with three channels which use different architectures.*



## Conclusion

Ce tour d'horizon montre qu'il existe de nombreux moyens permettant d'améliorer le niveau de sécurité d'un système à microprocesseur par application du concept de redondance.

Parmi toutes les méthodes citées, certaines sont à mettre en œuvre dès la conception du système alors que d'autres permettent d'améliorer un dispositif existant. Le concepteur ou l'utilisateur pourra donc choisir celle qui convient le mieux à son application selon des critères de coût, de facilité et de possibilité de mise en œuvre et des exigences de sécurité recherchées.

Quelle que soit la méthode retenue, on veillera à apporter les mêmes soins de réalisation au niveau des organes d'entrées-sorties, capteurs et actionneurs qu'au niveau de l'unité de traitement. L'organe de décision, comparateur ou voteur, devra être conçu en sécurité intrinsèque puisqu'il constitue la clé de voûte de toute architecture redondante.

Comme des énergies de plus en plus faibles sont capables de perturber les nouveaux circuits du fait de leur degré d'intégration de plus en plus grand, l'utilisation de la redondance ne dispense pas de l'application des règles de l'art en matière de conception : blindage, filtrage...

Une fois le système réalisé, il sera nécessaire de s'assurer que son niveau de sécurité est bien celui escompté. Pour cela, on procédera à des tests de qualification permettant d'observer le comportement du système en présence de défaillances. On pourra notamment avoir recours à la simulation physique de défauts au niveau du matériel et du logiciel. L'I.N.R.S. a d'ailleurs conçu un appareil permettant de réaliser ce type de test de façon automatique.

L'obtention de systèmes à haut niveau de sécurité n'est pas du domaine de l'utopie; la redondance est déjà utilisée dans des systèmes complexes nécessitant un très haut niveau de sécurité (nucléaire, aéronautique, spatial, transport...) : ce document montre que certaines méthodes de mise en œuvre de la redondance peuvent être appliquées dans l'industrie à des coûts raisonnables lorsque l'intégration de ce concept se fait dès la phase de conception.

Afin d'appréhender au mieux les travaux réalisés dans ce domaine, l'I.N.R.S. participe à un projet de collaboration entre sept organismes de la Communauté Européenne (R.F.A., Grande-Bretagne, Danemark et France) sur le thème « Évaluation, structure et fonctionnement des systèmes électroniques programmables industriels appliqués à la robotique »; les résultats de ce groupe de travail seront publiés en mai 1986 lors d'un congrès à Guernesey.